DEPARTMENT OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, DC 20301-6000

CHIEF INFORMATION OFFICER

NOV 0 2 2007

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
COMBATANT COMMANDERS
ASSISTANT SECRETARIES OF DEFENSE
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
DIRECTOR, OPERATIONAL TEST AND EVALUATION
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
ASSISTANTS TO THE SECRETARIES OF DEFENSE
DIRECTOR, ADMINISTRATION AND MANAGEMENT
DIRECTOR, PROGRAM ANALYSIS AND EVALUATION
DIRECTOR, NET ASSESSMENT
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTORS OF THE DOD FIELD ACTIVITIES

SUBJECT: Policy on Use of Department of Defense (DoD) Information Systems – Standard Consent Banner and User Agreement

This memorandum establishes interim policy on the use of DoD information systems. It requires the use of a standard Notice and Consent Banner and standard text to be included in user agreements. This memorandum supersedes the memorandum from ASD(C3I), "Policy on Department of Defense (DoD) Electronic Notice and Consent Banner," dated January 16, 1997. Conforming changes will be made to DoD Instructions and forms, relevant user agreements, and the DoD Web Site Administration Policies & Procedures.

The new banner at Attachment 1 shall be displayed at log on to all DoD information systems. (Choose either banner A or B based on the character limitations imposed by the system.) The banner is mandatory and deviations are not permitted except as authorized in writing by the DoD Chief Information Officer. The thrust of this new policy is to make it clear that there is no expectation of privacy when using DoD information systems and all use of DoD information systems is subject to searching, auditing, inspecting, seizing, and monitoring, even if some personal use of a system is permitted. The banner shall be implemented as a click-through banner at logon (to the extent permitted by the operating system), meaning it remains in place and prevents

further activity on the information system unless and until the user executes a positive action to manifest agreement by clicking on a box indicating "OK."

The language in Attachment 2 shall be included in all DoD information system user agreements. DoD components shall also conform component user agreements to this policy. A standardized DD form 2857, with the new language, is being studied and may be issued in the future.

This policy is not intended to negate any privilege recognized by law (e.g., attorney-client, psychotherapist-patient or clergyman-penitent privileges) with respect to communications over DoD information systems. To the extent such privileges would have existed and been recognized, but for the new banner and user agreement, this policy intends to effect no change.

This policy is effective immediately and shall be implemented no later than 40 days from the date of this memorandum. Any portion of component policy conflicting with this policy is superseded 40 days from the date of this memorandum unless the component obtains an extension through the POC listed below.

Use of the following measures to widely and effectively disseminate this new policy is encouraged:

1. Training, both initial in-processing of new personnel and annual security refresher training
2. Publication of this information in installation newspapers, daily bulletins, and other media to reemphasize this policy
3. Periodic security awareness briefings for all users

Additional information or assistance regarding this policy may be obtained from Mr. John Hunter, at john.hunter@osd.mil or 703-602-9927.

John G. Grimes

Attachments:
As stated

ATTACHMENT 1

STANDARD MANDATORY
DOD NOTICE AND CONSENT BANNER

[A. For desktops, laptops, and other devices accommodating banners of 1300 characters:]

~~You are accessing~~ a U.S. ~~Government (USG) information system (IS) that~~ is provided for USG-authorized use only.

By using this IS, you consent to the following conditions:

-The USG routinely monitors communications occurring on this IS, and any device attached to this IS, for purposes including, but not limited to, penetration testing, COMSEC monitoring, network defense, quality control, and employee misconduct, law enforcement, and counterintelligence investigations.
-At any time, the USG may inspect and/or seize data stored on this IS and any device attached to this IS.
-Communications occurring on or data stored on this IS, or any device attached to this IS, are not private. They are subject to routine monitoring and search.
-Any communications occurring on or data stored on this IS, or any device attached to this IS, may be disclosed or used for any USG-authorized purpose.
-Security protections may be utilized on this IS to protect certain interests that are important to the USG. For example, passwords, access cards, encryption or biometric access controls provide security for the benefit of the USG. These protections are not provided for your benefit or privacy and may be modified or eliminated at the USG's discretion.

OK

[B. For Blackberries and other PDAs/PEDs with severe character limitations:]

I've read & consent to terms in IS user agreem't.

ATTACHMENT 2

STANDARD MANDATORY NOTICE AND CONSENT PROVISION
FOR ALL DOD INFORMATION SYSTEM USER AGREEMENTS

By signing this document, you acknowledge and consent that when you access Department of Defense (DoD) information systems:

- You are accessing a U.S. Government information system (as defined in CNSSI 4009) that is provided for U.S. Government-authorized use only.

- You consent to the following conditions:

    - The government routinely monitors communications occurring on this information system, and any device attached to this information system, for purposes including, but not limited to, penetration testing, communications security (COMSEC) monitoring, network defense, quality control, employee misconduct investigations, law enforcement investigations, and counterintelligence investigations.
    - At any time, the government may inspect and/or seize data stored on this information system and any device attached to this information system.
    - Communications occurring on or data stored on this information system, or any device attached to this information system, are not private. They are subject to routine monitoring and search.
    - Any communications occurring on or data stored on this information system, or any device attached to this information system, may be disclosed or used for any U.S. Government-authorized purpose.
    - Security protections may be utilized on this information system to protect certain interests that are important to the government. For example, passwords, access cards, encryption or biometric access controls provide security for the benefit of the government. These protections are not provided for your benefit or privacy and may be modified or eliminated at the government's discretion.